

10 TÉRMINOS EN CIBERSEGURIDAD

QUE TODOS ESCUCHAN
PERO POCOS ENTIENDEN



1. DAEMON

Programa que corre en segundo plano en un equipo, sin que lo abras ni lo veas en la pantalla



Se encargan de tareas invisibles

2. BOTNET



Red de miles de ordenadores infectados que un atacante controla de forma remota sin que los usuarios lo sepan.

Se usan para lanzar ataques masivos (DDoS), enviar spam o robar datos.

Algunas botnets llegaron a controlar más de 1 millón de equipos.

3. HONEYPOT

Sistema trampa que simula ser un objetivo atractivo (como un servidor vulnerable) para atraer a los hackers y estudiarlos.



Puede tener datos falsos como tarjetas de crédito para engañar al atacante

4. PAYLOAD

Parte del malware que realiza la acción dañina como cifrar archivos, robar contraseñas o abrir una puerta de acceso al atacante



Muchos virus esperan “dormidos” hasta activarlo.

5. PHISHING

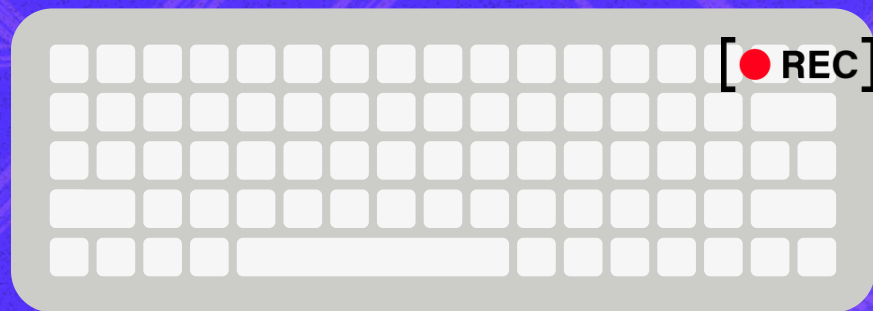
Engaño donde un atacante se hace pasar por alguien de confianza para robar información sensible.



El 90% de los ataques cibernéticos en empresas comienzan con phishing.

6. KEYLOGGER

Programa que registra todo lo que escribes en el teclado. Los hackers lo usan para obtener información privada sin que lo notes.



Usar teclado en pantalla o 2FA puede arruinarles el plan

7. RAMSONWARE

Malware que cifra tus archivos o bloquea sistemas y pide un rescate (dinero) a cambio de recuperarlos



WannaCry paralizó hospitales y empresas en 2017

8. SPOOFING

Suplantación de identidad digital donde un atacante finge ser otro dispositivo o servidor.

Engaña sistemas, falsifica mensajes o redirige tráfico, sin robar datos.



Puede hacer que tu PC participe en ataques sin que lo notes

9. BACKDOOR

Puerta trasera en un sistema que permite entrar sin pasar por los controles normales, como contraseñas o firewalls



Algunos incluso permiten que los atacantes controlen todo el sistema.

10. ZERO-DAY

Vulnerabilidad desconocida que aún no tiene parche. Los hackers pueden usarla para atacar sin que nadie pueda defenderse.



El gusano Stuxnet usó 4 zero-days diferentes

BONUS SCRIPT KIDDIE

Persona que se hace pasar por hacker, pero solo usa herramientas creadas por otros, sin entender cómo funcionan.



Muchos se delatan porque dejan rastros
obvios en sus ataques



Saúl Ruiz

¡Guarda este post para repasarlo
cuando quieras!

